U.S. DEPARTMENT OF HOUSING AND URBAN DEVLEOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
"CITIZEN-ACCESS WEB INTERFACE PROTOTYPE TO THE CREDIT ALERT SYSTEM (FORMERLY CREDIT ALERT INTERACTIVE VOICE RESPONSE SYSTEM – CAIVRS)"
(OMB Unique Identifier: N/A and PCAS # 251440)
January 11, 2005

NOTE: See Section 2 for PIA answers, and Section 3 for Privacy Advocate's determination.

SECTION 1: BACKGROUND

Importance of Privacy Protection – Legislative Mandates:
HUD is responsible for ensuring the privacy and confidentiality of the information it collects on members of the public, beneficiaries of HUD programs, business partners, and its own employees. These people have a right to expect that HUD will collect, maintain, use, and disseminate identifiable personal information only as authorized by law and as necessary to carry out agency responsibilities.

The information HUD collects is protected by the following legislation and regulations:

- Privacy Act of 1974, as amended affords individuals the right to privacy in records that are maintained and used by Federal agencies. (See http://www.usdoj.gov/foia/privstat.htm; see also HUD Handbook1325.1 at www.hudclips.org);
- Computer Matching and Privacy Protection Act of 1988 is an amendment to the Privacy Act that specifies the conditions under which private information may (or may not) be shared among government agencies. (See http://www.usdoj.gov/foia/privstat.htm);
- Freedom of Information Act of 1966, as amended (http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm) provides for the disclosure of information maintained by Federal agencies to the public, while allowing limited protections for privacy. See also HUD's Freedom of Information Act Handbook (HUD Handbook 1327.1 at www.hudclips.org);
- E-Government Act of 2002 requires Federal agencies to conduct Privacy Impact Assessments (PIAs) on its electronic systems. (See http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf; see also the summary of the E-Government Act at http://www.whitehouse.gov/omb/egov/pres_state2.htm);
- Federal Information Security Management Act of 2002 (which superceded the Computer Security Act of 1987) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, etc. See also the codified version of Information Security regulations at Title 44 U.S. Code chapter 35 subchapter II (http://uscode.house.gov/search/criteria.php); and

- OMB Circular A-130, Management of Federal Information Resources, Appendix I (http://www.whitehouse.gov/omb/circulars/a130/appendix_i.pdf) defines Federal Agency responsibilities for maintaining records about individuals.

Access to personally identifiable information will be restricted to those HUD staff that have been authorized because of their duties; and they will be held accountable for ensuring privacy and confidentiality.

What is the Privacy Impact Assessment (PIA) Process?
The Privacy Impact Assessment (PIA) is a process that evaluates issues related to the privacy of personally identifiable information in electronic systems. See background on PIAs and the 7 questions that need to be answered, at: http://www.hud.gov/offices/cio/privacy/pia/pia.cfm. Personally identifiable information is defined as information that actually identifies an individual, e.g., name, address, social security number (SSN), or identifying number or code; or other personal/ sensitive information such as race, marital status, financial information, home telephone number, personal e-mail address, etc. Of particular concern is the combination of multiple identifying elements. For example, knowing name + SSN or name + date of birth + financial information would pose more risk to privacy than just name + date of birth alone.

The PIA:
- Identifies the type of personally identifiable information in the system (including any ability to combine multiple identifying elements on an individual);
- Identifies who has access to that information (whether full access or limited access rights); and
- Describes the administrative controls that ensure that only information that is necessary and relevant to HUD's mission is included.

Who Completes the PIA?
Both the program area system owner and IT project leader work together to complete the PIA. The system owner describes what personal data types are collected, how the data is used, and who has access to the personal data. The IT project leader describes whether technical implementation of the system owner's requirements presents any risks to privacy, and what controls are in place to restrict access of personally identifiable information.

When is a Privacy Impact Assessment (PIA) Required?

1. New Systems: Any new system that will contain personal information on members of the public requires a PIA, per OMB requirements (this covers both major and non-major systems).

2. Existing Systems: Where there are significant modifications involving personal information on members of the public, or where significant changes been made to the system that may create a new privacy risk, a PIA is required.

3. Information Collection Requests, per the Paperwork Reduction Act (PRA): Agencies must obtain OMB approval for new information collections from ten or more

members of the public. If the information collection is both a new collection and automated, then a PIA is required.

Privacy Act. The Privacy Act of 1974, as amended (http://www.usdoj.gov/foia/privstat.htm) requires that agencies publish a Federal Register Notice for public comment on any intended information collection. Privacy Act Systems of Records are created when information pertaining to an individual is collected and maintained by the Department, and is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned to an individual. The E-Government Act of 2002 requires PIAs for electronic systems as well as information collection requests that are automated. So, there is a relationship between the new PIA requirement (when automation is involved) and the long-standing Privacy Act System of Records Notices (for both paper-based and automated records that are of a private nature). For additional information, contact the Departmental Privacy Act Officer in the Office of the Chief Information Officer.

Publication of PIA summary. The E-Government Act of 2002 requires that the analysis and determinations resulting from the PIA be made publicly available. The Privacy Advocate in HUD's Office of the Chief Information Officer (OCIO) is responsible for publishing the PIA summary on HUD's web site. See: http://www.hud.gov/offices/cio/privacy/pia/pia.cfm.

SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT

Please submit answers to the Departmental Privacy Advocate in the Office of the Chief Information Officer (OCIO). If any question does not apply, state Not Applicable (N/A) for that question, and briefly explain why it is not applicable.

Program Area: U.S. Department of Housing and Urban Development (HUD), Office of Single Family Housing

NOTE: HUD has the lead with CAIVRS, but data is contributed by other Federal credit agencies. CAIVRS is used by lenders who issue loans under the following Federal agencies' loan programs: HUD's Federal Housing Administration (HUD-FHA), Veterans Affairs (VA), U.S. Department of Agriculture (USDA), Small Business Administration (SBA), and Department of Education. CAIVRS is also used by the Department of Justice (DOJ).

Subject matter expert in the program area: Richard J. Bradley, Housing Program/ Policy Specialist, Home Mortgage Insurance Division, Office of Single Family Program Development, HUD, 202-708-2121 ext. 2326

Program area manager: James A. Beavers, Director, Home Mortgage Insurance Division, Office of Single Family Program Development, HUD, 202-708-2121 ext. 2205

IT Project Leader: Sheila Alpers, Computer Specialist, Office of the Chief Information Officer, HUD, 202-708-1587 ext. 7610; and Allen Correll, Office of the Chief Information Officer, HUD, 202-708-5495 ext. 6671

For IT Systems:

- **Name of system:** Citizen-access web interface prototype of HUD's Credit Alert System (formerly Credit Alert Interactive Voice Response System – CAIVRS)
- **PCAS #:** 251440
- **OMB Unique Project Identifier # (if submitting an Exhibit 300 to OMB):** N/A (not a major system, therefore an Exhibit 300 was not submitted to OMB)

For Information Collection Requests:

- **Name of Information Collection Request:**
- **OMB Control #:**

Question 1: Provide a brief description of what information is collected.

Each month, the participating agencies listed above transmit via secure file transfer protocol (FTP) the following data on borrowers who have defaulted on loans administered by that agency: Social Security Number/ Employee Identification Number (SSN/EIN), case number, Federal Agency identifying code, and record type. DOJ also provides data to CAIVRS, even though DOJ does not administer loan programs.

Currently, when authorized lenders and Federal agency staff access CAIVRS (either via the telephone voice response system or the new web-based interface), they enter a user authorization code, an SSN/EIN, and CAIVRS returns the following data:

- Yes/ No as to whether the holder of that SSN/EIN is in default on a Federal loan; and

- If Yes, then CAIVRS provides to the lender:
  - Loan case number;
  - Record type (claim, default, foreclosure, or judgment);
  - Agency administering the loan program; and
  - Phone # at that agency (to call to clear up the default)

  Please note that SSN/EIN is not returned in response to the query – only the 4 elements above are returned. Also, name of borrower is not even in the CAIVRS database so cannot be displayed.

For the proposed citizen-access web interface prototype, the same information will be provided to the person entering his/ her own SSN; namely:

- Yes/ No as to whether the person holding that SSN is in default on a Federal loan; and
- If Yes, then CAIVRS will provide to the citizen:
  - Loan case number;
  - Record type (claim, default, foreclosure, or judgment);
  - Agency administering the loan program; and
  - Phone # at that agency (to call to clear up the default)

  Please note that SSN is not returned in response to the query – only the 4 elements above are returned. Also, name of borrower is not even in the CAIVRS database so cannot be displayed.

If this automated system (or Information Collection Request) involves personally identifiable information on members of the public, then mark any of the categories that apply below:

NOTE: As of November 30, 2004, the CAIVRS database currently holds the SSN/EINs of 2,136,106 borrowers who are in default on a Federal loan. Borrowers' names associated with the SSN/EINs are not transmitted by the agencies to CAIVRS. 85,331 lenders currently have a user ID and password to check CAIVRS for a "match" on a potential borrower's SSN/EIN ("Yes/ No" as to whether that person – or more precisely, the SSN/EIN since names of persons are not contained in CAIVRS – has defaulted on any Federal loan). The following data elements are contained in the CAIVRS database, but none of these are returned to the lender (or to the citizen for the citizen-access prototype) in response to a query. Only the information listed above is returned.

Personal Identifiers:

	Name: No borrower or co-borrower names are stored in CAIVRS
X	Social Security Number (SSN)
X	Other identification number (specify type): Case number of the loan
	Birth date
	Home address
	Home telephone
	Personal e-mail address
	Fingerprint/ other "biometric"
	Other (specify):
	None

	Comment:

Personal/ Sensitive Information:

	Race/ ethnicity
	Gender/ sex
	Marital status
	Spouse name
	# of children
	Income/ financial data (specify type of data, such as salary, Federal taxes paid, bank account number, etc.):
	Employment history
	Education level
	Medical history/ information
	Disability
	Criminal record
X	Other (specify): Agency administering the loan program + record type (claim, default, foreclosure or judgment) and telephone number at that agency (to clear the default)
	None
	Comment:

Question 2: Type of electronic system or information collection. Fill out Section A, B, or C as applicable.

A. If a new electronic system (or one in development): Is this a new electronic system (implemented after April 2003, the effective date of the E-Government Act of 2002)?

	Yes
X	No

NOTE: Although CAIVRS was implemented in 1988, the citizen-access web interface prototype is new. It will expand access to CAIVRS data beyond lenders to the citizens themselves, with the goal of helping to clear the massive amount of defaulted Federal loans.

B. If an existing electronic system: Mark any of the following conditions for your existing system that OMB defines as a "trigger" for requiring a PIA (if not applicable, mark N/A):

	Conversion: When paper-based records that contain personal information are converted to an electronic system
	From Anonymous (Non-Identifiable) to "Non-Anonymous" (Personally Identifiable): When any systems application transforms an existing database or data collection so that previously anonymous data becomes personally identifiable
	Significant System Management Changes: When new uses of an existing electronic system significantly change how personal information is managed in the system. (Example #1: when new "relational" databases could combine multiple identifying data elements to more easily identify an individual. Example #2: when a web portal extracts data elements from separate databases, and thereby creates a more open environment for exposure of personal data)

	Merging Databases: When government databases are merged, centralized, matched, or otherwise significantly manipulated so that personal information becomes more accessible (with special concern for the ability to combine multiple identifying elements)
X	**New Public Access:** When new public access is given to members of the public or to business partners (even if the system is protected by password, digital certificate, or other user-authentication technology) For the citizen-access prototype, the individual puts in a Social Security Number (SSN) to find out if that SSN is associated with a Federal loan that is in default (Yes/ No). If yes, then the only information that is returned in response to the query of CAIVRS is the name of the Federal agency administering the loan program, the agency-assigned case number, record type (claim, default, foreclosure, or judgment) and a telephone number at that agency (to clear the default). The person's SSN is never displayed, and the name of the borrower cannot be accessed because it is not even contained in the CAIVRS database.
	Commercial Sources: When agencies systematically incorporate into databases any personal data from commercial or public sources (ad hoc queries of such sources using existing technology does not trigger the need for a PIA)
	New Inter-agency Uses: When agencies work together (such as the federal E-Gov initiatives), the lead agency should prepare the PIA
	Business Process Re-engineering: When altering a business process results in significant new uses, disclosures, or additions of personal data
	Alteration in Character of Data: When adding new personal data raises the risks to personal privacy (for example, adding financial information to an existing database that contains name and address)

C. If an Information Collection Request (ICR): Is this a new Request that will collect data that will be in an automated system? Agencies must obtain OMB approval for information collections from 10 or more members of the public. The E-Government Act of 2002 requires a PIA for ICRs only if the collection of information is a new request and the collected data will be in an automated system.

	Yes, this is a new ICR and the data will be automated
X	No, the ICR does not require a PIA because it is not new or automated)

Question 3: Why is the personally identifiable information being collected? How will it be used? Mark any that apply:

Homeownership:

	Credit checks (eligibility for loans)
	Loan applications and case-binder files (via lenders) – including borrower SSNs, salary, employment, race, and other information
	Loan servicing (MIP collections/refunds and debt servicing for defaulted loans assigned to HUD)
	Loan default tracking
X	Issuing Mortgage and loan insurance.

X	Other (specify): Managing loan guarantee risks
X	Comment: CAIVRS ensures that HUD/FHA and the Federal lending community remain in compliance with the following legislation and guidance: • Title 31, United States Code, Section 3720B, Public Law 100-503; • Office of Management and Budget (OMB) Circulars A-129 and A-70; • Budget and Accounting Acts of 1921 and 1950, as amended; • Debt Collection Act of 1982, as amended; • Deficit Reduction Act of 1984, as amended, • Debt Collection Improvement Act of 1996, as amended; the Federal Claims Collection Standards Act of 1998.

Rental Housing Assistance:

	Eligibility for rental assistance or other HUD program benefits
	Characteristics on those receiving rental assistance (for example, race/ethnicity, # of children, age)
	Property inspections
	Other (specify):
	Comment:

Grants:

	Grant application scoring and selection – if any personal information on the grantee is included
	Disbursement of funds to grantees – if any personal information is included
	Other (specify):
	Comment:

Fair Housing:

	Housing discrimination complaints and resulting case files
	Other (specify):
	Comment:

Internal operations:

	Employee payroll or personnel records
	Payment for employee travel expenses
	Payment for services or products (to contractors) – if any personal information on the payee is included
	Computer security files – with personal information in the database, collected in order to grant user IDs
	Other (specify):
	Comment:

Other lines of business (specify uses):

X	Eligibility for new HUD, VA, SBA, USDA loans
X	Tool for collecting defaulted loans
X	Compliance screening of non-government personnel for positions of trust in

	implementation of Federal credit programs

Question 4: Will you share the information with others (e.g., another agency for a programmatic purpose, or outside the government)? Mark any that apply:

X	Federal agencies? (specify): CAIVRS data is provided by HUD, VA, USDA, SBA, Education, and DOJ; and used by Federal agency employees and lenders who are authorized to issue loans under those agencies' loan programs – to determine if the loan applicant defaulted on a prior Federal loan, and/ or to collect on defaulted debts.
	State, local, or tribal governments?
	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
X	FHA-approved lenders?
	Credit bureaus?
	Local and national organizations?
	Non-profits?
	Faith-based organizations?
	Builders/ developers?
	Others? (specify):
X	Comment: Self only. If the citizen-access web interface prototype is implemented, then citizens could check only on their own Federal debt status. They would have to provide SSN and some other identifying information to prove that the person requesting information on an SSN is the person who owns that SSN.

Question 5: Can individuals "opt-out" by declining to provide personal information or by consenting only to particular use (e.g., allowing their financial information to be used for basic rent eligibility determination, but for not for sharing with other government agencies)?

	Yes, they can "opt-out" by declining to provide private information or by consenting only to particular use
X	No, they can't "opt-out" – all personal information is required
X	Comment: The only item required for a query to CAIVRS is the SSN – which then brings up a Yes/ No answer as to whether the SSN is associated with a defaulted Federal loan or a federal claim payment. No personal-identifiable information is returned in answer to a query.

If Yes, please explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data): _____
_____

Question 6: How will the privacy of the information be protected/ secured? What are the administrative and technological controls? Mark any that apply and give details if requested:

X	System users must login with a password: Federal employees and approved lenders must use individually assigned User ID and password to access CAIVRS.
X	When an employee leaves: • How soon is the user ID terminated (1 day, 1 week, 1 month, unknown)? The CAIVRS administrator terminates user IDs immediately upon receipt of a request from the appropriate manager in the relevant agency/ program. • How do you know that the former employee no longer has access to your system? (Explain your procedures or describe your plan to improve): Twice each year, the CAIVRS administrator contacts appropriate managers for each agency/ program to recertify all employees who are to have access to CAIVRS. Specifically, they certify that those employees are still at the agency, and it is still within their authorized duties to have system access.

X
 	
X
	Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the approximate # of authorized users who have either:
	• Full access rights to all data in the system (specify number)? 4 NOTE: Full access rights to CAIVRS include rights to: inquiry functions, maintenance functions, agency administrator functions, and system administrator functions.
	• Limited/ restricted access rights to only selected data (1-10, 20-100, over 100)? NOTE: Limited access means only inquiry access to borrower information; namely the 5 data elements returned by a query to CAIVRS, which are "Yes/ No" and if yes then loan number, record type, agency, and phone # at that agency.
	  o 87,698 lenders (as of Sept. 2004) have inquiry access to CAIVRS. If the citizen-access web interface prototype is implemented, then any individual could check for their own record in CAIVRS – by entering their own SSN and some other identifying information (such as birthdate). Currently, 2.1 million SSNs would return a "match" from CAIVRS, indicating those who are in default on a Federal loan.
	  o Federal agency staff also have query access to CAIVRS, similar to that by lenders described above.
	  o If the debt has been satisfied (is no longer delinquent) or an error has been made in reporting to CAIVRS, specific authorized program official(s) from the reporting agency can suppress CAIVRS reporting of the borrower's record. A limited number of Program Official(s) within each agency have been granted special privileges (over and above inquiry access) and a PIN (personal identification number) by the CAIVRS administrator to suppress CAIVRS reporting. The program official must provide the reason for the suppression (such as reporting error or debt paid), and in the case of funds being paid must specify the amount collected and the manner in which it was collected (i.e., partial payment, payment in full, IRS offset, etc). An audit trail of all CAIVRS suppressions is kept indefinitely by the system, and is available for reporting.

X	Are disks, tapes, and printouts that contain personal information locked in cabinets when not in use? (Explain your procedures, or describe your plan to improve):

	Not Applicable – data is sent electronically and is overwritten monthly. No printouts are maintained in the office.
	If data from your system is shared with another system or data warehouse, who is responsible for protecting the privacy of data that came from your system but now resides in another? Explain the existing privacy protections, or your plans to improve:
X	If data from another system or data warehouse is shared with (input to) your system, who is responsible for protecting the privacy of data that came from those systems and now resides in your system? Explain the existing privacy protections, or your plans to improve: • HUD has signed computer matching agreements with all federal agencies that provide data to CAIVRS, per the Privacy Act of 1974 as amended. • The HUD data sent to CAIVRS is extracted from HUD's Computerized Homes Underwriting Management System (CHUMS – F17) and FHA Connection (FHAC – F17C). The Office of Housing security administrators for those source systems are responsible for having adequate user authentication processes that restrict loan application data to authorized users of CHUMS and FHA Connection. The other agencies that provide data to CAIVRS (Education, SBA, USDA, and VA) are responsible for having adequate user authentication processes that restrict loan application data to authorized users of their source systems.
	Other methods of protecting privacy (specify):
	Comment:

Question 7: If private information is involved, by what data elements can it be retrieved?
Mark any that apply:

NOTE: Even though other data elements are contained in the CAIVRS database (as described in Question 1), the only way that a "match" on a defaulted loan is determined is by entering an SSN into the CAIVRS web site.

	Name
X	Social Security Number (SSN)
	Identification number (specify type):
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
	Home address
	Home telephone
	Personal e-mail address
	Other (specify):
	None
X	Comment: SSN is the only private data element in CAIVRS, and is the only way that data can be retrieved from CAIVRS. The SSN is entered, and CAIVRS

	searches the database for a "match" on the SSN. No information is returned if there is no match. If a match is found ("Yes" as to whether there is a defaulted Federal loan), then the name of the Federal agency, the agency-assigned case number, record type (claim, default, foreclosure or judgment) and an agency telephone number to call for more information or to clear the default.

Other Comments (or details on any Question above):

SECTION 3: DETERMINATION BY HUD PRIVACY ADVOCATE

At first it would seem that the citizen access web interface to CAIVRS would be a major privacy concern, because of the mention of 2.1 million Social Security Numbers (SSNs).

However, in analyzing the details of the data included in the system, and the restricted method of returning answers to queries, this is much less of a concern for privacy. The CAIVRS data base does not include any borrower names, so the SSNs cannot be matched up with any other personally identifiable information. Only 4 data elements are returned for those SSNs that give a "match" as to a loan in default: If Yes, then CAIVRS will provide to the citizen:

- Loan case number;
- Record type (claim, default, foreclosure, or judgment);
- Agency administering the loan program; and
- Phone # at that agency (to call to clear up the default)

It is significant that neither SSN/EIN nor name of the borrower is returned in response to the query – only the 4 elements above are returned.

The method of "authenticating" the citizen making a query on his or her SSN is still being considered for the prototype. http://www.pay.gov/ is being investigated as a prime option, upon recommendation of the GSA E-Authentication technical team. Whatever method is adopted will be knowledge-based. In addition to having to know the SSN to do a match on the CAIVRS database, the person would have to type in some other identifying information that could be matched against a database such as http://www.pay.gov/ uses: Optional "identifying" information to allow access to the CAIVRS data include:

- Birthdate (in addition to the SSN); or
- Last name and first name (in addition to the SSN); or
- ZIP code of current address (in addition to the SSN); or
- Two or more of the items above, depending on the level of concern for authenticating that the SSN entered actually belongs to the person coming to the citizen-access web interface to CAIVRS.

Once the citizen "authentication" method has been selected (whether www.Pay.gov or some other method), the CAIVRS managers should request a final determination by the HUD Privacy Advocate before actual implementation of the prototype.

/signed/ January 11, 2005

Eric M. Stout
Privacy Advocate,
Office of the Chief Information Officer
U.S. Department of Housing and Urban Development

date